

### **REMARKS**

Applicant has cosmetically amended the specification to correct minor typographical errors. No new matter has been added. Applicant believes that the following comments and remarks will convince the Examiner that the rejections set forth in the September 27, 2004 Office Action have been overcome and should be withdrawn.

#### **I. THE INVENTION**

Generally, the present invention is a system and method for providing secure communication over a network. The present invention assures privacy over an insecure network and provides a confirmation that a given message was received by the intended recipient or recipients. The present invention further discloses the novel use of potentially destructive algorithms and instructions to discourage tampering and interception of transmitted messages. The sender of an electronic message includes within the transmission a set of potentially harmful instructions (e.g., delete all files in the working directory) to be executed upon interception or failed decryption of a message secured by the present invention. Thus, tampering and interception is reduced because of the

threat of damage to a potential interceptor's system. Several other safeguards for protecting a given message are also disclosed.

## II. THE EXAMINER'S REJECTIONS

### A. 35 U.S.C. § 102(e)

The Examiner rejected claims 1, 2, 7, 8, 13, and 14 under 35 U.S.C. § 102(e) as being anticipated by Wray et al. U.S. Patent No. 6,442,696 (hereinafter referred to as "Wray"). Without enumerating the claim limitations, the Examiner opined that Wray "discloses these features" contained in the abovementioned claims (September 27, 2004 Office Action, p. 2).

### B. 35 U.S.C. § 103(a)

The Examiner rejected claims 3-6, 9-12, and 15-18 under 35 U.S.C. § 103(a) as being unpatentable over Wray in view of the Examiner taking official notice. The Examiner admitted that Wray fails to disclose the limitations disclosed in claims 3, 9, and 15; however, the Examiner contended that "[i]t would have been obvious to anyone having an ordinary level of skill in the art at the time the invention was made to have included [these] features in the invention of Wray et al. since this information should

be known to all parties in order that the situation can be corrected." (September 27, 2004 Office Action, p. 3)

Per claim 4, the Examiner also conceded that Wray does not disclose the use of a list containing authorized users. The Examiner argued, however, that the use of a list is obvious "since it increases the level of security and provides a simple method of identifying authorized users." (September 27, 2004 Office Action, p. 3)

With regard to claims 5, 11, and 17, the Examiner again conceded that Wray fails to disclose the use of biometric identifiers as the identifying user information. The Examiner opined, however, that "this is a well known method of identification." (September 27, 2004 Office Action, p. 3)

Lastly, the Examiner rejected the remaining claims 6, 10, 12, 16, and 18 "for the same reason as stated in the statement of claim 4." (September 27, 2004 Office Action, p. 3)

### III. THE EXAMINER'S REJECTIONS SHOULD BE WITHDRAWN

#### A. 35 U.S.C. § 102(e)

The Examiner rejected claims 1, 2, 7, 8, 13, and 14 under 35 U.S.C. § 102(e) as being anticipated by Wray. Applicant respectfully disagrees. Specifically, Wray does

not disclose the use of "an instruction set that is executed by a receiving computer when a predetermined condition is met" and "disabled upon verification of identifying user information." This limitation is present in all base claims 1, 7, and 13 and is part of the novelty of the present invention. Communication protected with the present system includes an instruction set within the protected communication so that an attempt to access the communication by an unauthorized user results in the execution of the instruction set affecting the unauthorized user's system. For example, the instruction set could notify a secure server of the unsuccessful access attempt, delete the communication from the user's computer, or cause damage to the unauthorized user's system. It is well known that the threat of harm to oneself or one's property is a powerful deterrent. In relation to the present invention, the consequences of a would-be eavesdropper attempting decryption of a protected message are specified by the sender of the protected message contained in an instruction set embedded in the encrypted message. This attempted access of the message results in certain consequences such as damage to the eavesdropper's system. Thus, potential eavesdroppers must decide whether to ignore or heed this threat before attempting to access the protected message.

Further, the claimed invention discloses the novel disabling of the potentially destructive instruction set upon "verification of identifying user information." This element is also included in each base claim 1, 7, and 13. A recipient of a protected message has the option to "defuse" the message, or to remove the potentially damaging instruction set from the message. Since Wray does not disclose the use of a potentially damaging instruction set in response to a request for a secure communication, Wray does not contemplate or even suggest the disabling of this instruction set.

Wray discloses a system that can carry out generic instructions from a host after a relationship between a host and client is established (see col. 13, line 65 - col. 14, line 11). Typically, these instructions are remote administration instructions or instructions to simply reply to a server with the client's unique key. These instructions are in stark contrast to the instruction set embedded in protected messages of the claimed invention. Namely, Wray's instructions are not "in response to a request for secure communication" and are not "disabled upon verification of the identifying user information" as required by base claims 1, 7, and 13.

Applicant respectfully submits that Wray does not disclose each and every element of base claims 1, 7, and 13 and therefore does not anticipate these claims or claims 2, 8, and 14 dependent thereon.

B. 35 U.S.C. § 103(a)

The Examiner rejected claims 3-6, 9-12, and 15-18 under 35 U.S.C. § 103(a) as being unpatentable over Wray in view of the Examiner taking official notice. Applicant respectfully disagrees. As argued above for the rejection of the base claims 1, 7, and 13 under 35 U.S.C. § 102(e), Wray does not disclose each and every limitation of the claimed invention. Hence dependent claims 3-6, 9-12, and 15-18 cannot be unpatentable over any combination of Wray and the Examiner's official notice.

Wray teaches a client identification system that uses detailed system configuration information to create a unique system signature, or key. This key, when requested by a server, is sent from a client to the requesting server. If the client has no relationship with the server, the server ignores the client's key. If the client has a relationship with the requesting server, the server responds by sending custom pages of information to the client.

This process is quite dissimilar to the claimed invention, which associates a potentially damaging instruction set with a secure communication so as to deter unauthorized access or interception of the communication. Conversely, Wray's system is concerned with client identification and the delivery of pages of data matched to a requesting client. Wray does not disclose a deterrent for unauthorized access of a protected page of data, the execution of a potentially harmful instruction set on an unauthorized system, or the disabling of such instruction set.

Applicant respectfully submits that none of the claims 3-6, 9-12, and 15-18 are obvious in view of Wray as suggested by the Examiner. In order for a claimed invention to be obvious in view of a combination of references: 1) there must exist a suggestion or motivation to modify the reference or to combine reference teachings; 2) there must be a reasonable expectation of success; and 3) the prior art references, when combined, must teach or suggest all of the claim limitations (see *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991) and also Manual of Patent Examining Procedure §§ 2143-2143.03). The prior art reference(s) do not teach or even suggest all of the claim limitations of the claimed invention.

While the Examiner takes official notice that systems for providing information to all users of the system, systems allowing authorized users to access the system, and systems capable of recognizing users are known in the art, the Examiner fails to identify any such systems known in the art at the time of the invention. Applicant respectfully traverses the Examiner's taking of official notice as it is unclear as to the Examiner's basis for taking official notice. Applicant therefore requests that the Examiner identify references teaching such systems and identify the suggestion or motivation to combine such references (see Manual of Patent Examining Procedure § 2144.03). Even if such systems are known, the Examiner does not point to any suggestion or motivation in the references themselves to combine these teachings or demonstrate any reasonable expectation of success in combining these references at the time of the invention.

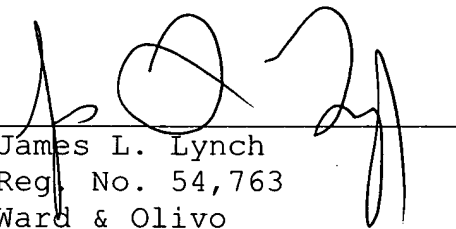
In view of the foregoing, Applicant requests that the rejection of claims 3-6, 9-12, and 15-18 be reconsidered and withdrawn. Applicant submits that the invention as claimed in these claims is not unpatentable over any combination of Wray and the Examiner's official notice.



**CONCLUSION**

Applicant submits that all pending claims represent a patentable contribution to the art and are in condition for allowance. No new matter has been added. Early and favorable action is accordingly solicited.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'J. Lynch', is written over a horizontal line.

James L. Lynch  
Reg. No. 54,763  
Ward & Olivo  
382 Springfield Ave.  
Summit, NJ 07901  
908-277-3333

Date: January 27, 2005